Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 21 April 2004

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Boston Herald reports the Bank of America is reissuing Fleet Visa business credit cards after an attack by hackers who possibly got hold of sensitive card numbers via a merchant's computer system. (See item 7)

- The Los Angeles Times reports health officials have confirmed that a Westchester County, New York, man was infected with a strain of flu that normally affects birds, only the second such case reported in the United States. (See item 17)

- The Washington Post reports computer security experts in the U.S. and UK confirmed Tuesday that an inherent design flaw in TCP could make it easy for hackers to disrupt Internet communications worldwide. (See item 24)

- The Associated Press reports a gasoline tanker truck has been missing from a Pennsauken, NJ, parking lot for more than a week and the New Jersey Office of Counterterrorism has asked all the state's law enforcement agencies to look for the truck. (See item 29)

- Security Focus has raised ThreatCon to Level 2, citing a need for increased vigilance. Please refer to the Internet Alert Dashboard.

DHS/IAIP Update *Fast Jump*

Production Industries: **Energy**; **Chemical**; **Defense Industrial Base**

Service Industries: **Banking and Finance**; **Transportation**; **Postal and Shipping**

Sustenance and Health: **Agriculture**; **Food**; **Water**; **Public Health**

Federal and State: **Government**; **Emergency Services**

IT and Cyber: **Information and Telecommunications**; **Internet Alert Dashboard**

Other: **General**; **DHS/IAIP Web Information**

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *April 20, Associated Press* — **Energy leaders look to spark new ideas. Faced with growing unrest over power shortages in the Western Hemisphere, energy ministers from more than 30 countries held a summit Tuesday, April 20, to discuss alternative energy exploration and ways to spur energy investment.** The two−day summit drew Secretary of Energy Spencer Abraham and dozens of other leaders from the Western Hemisphere. The United States is projected to significantly increase its reliance on energy imports in coming years, according to the U.S. Energy Information Administration. **With little investment in alternative energy such as solar and wind power, the United States remains heavily dependent on the Organization of Petroleum Exporting Countries.** "If the U.S. doesn't diversify its mix, all of these things are kind of rearranging deck chairs on the Titanic," said Daniel Kammen, a professor at the University of California, Berkeley, who specializes in energy. Some analysts say liquefied natural gas (LNG), currently a small portion of natural gas consumption in the United States, will continue to grow quickly as a source of energy throughout the world. The summit's host, Trinidad and Tobago, has invested heavily in LNG and supplied the United States with more than 75 percent of its LNG imports last year.
Source: http://edition.cnn.com/2004/WORLD/americas/04/20/energy.summ it.ap/

2. *April 20, Reuters* — **Libya welcomes signs of an end of U.S. sanctions.** Libya welcomed on Tuesday, April 20, indications that the United States could lift many economic sanctions soon, saying it would spur investment from U.S. and other international companies. **U.S. officials said on Monday, April 19, that sanctions barring U.S. businesses from investing in and buying Libyan oil could be ended this week, but they cautioned that time frame could slip.** Ties between Washington and the oil−producing North African state have improved since Libya last year said it would give up weapons of mass destruction and agreed to compensate victims of a 1988 plane bombing. U.S. officials said the main sanctions imposed on Libya under the International Emergency Economic Powers Act and the Iran−Libya Sanctions Act were expected to be removed soon. Among the biggest beneficiaries would be the U.S. oil companies in the Oasis Group of Marathon Oil Co., Amerada Hess, and ConocoPhillips, which were forced out of Libya by the U.S. sanctions in 1986. **U.S. oil companies have been eager to return to their Libyan holdings, some of which are due to expire in the coming years, amid concern they could lose some interests to European competitors not bound by the sanctions.**
Source: http://biz.yahoo.com/rc/040420/libya_sanctions_1.html

[Return to top]

Chemical Sector

Nothing to report.

[Return to top]

Defense Industrial Base Sector

3.

April 20, Government Computer News — **DoD considers creation of national software security lab.** Department of Defense (DoD) cybersecurity managers are urging Secretary of Defense Donald Rumsfeld to establish a high−assurance software lab serving all of DoD. The lab would be virtual, drawing on the existing software certification capabilities scattered across DoD research facilities. Joe Jarzombek, deputy director for software assurance in DoD's Information Assurance Directorate, said **the measure is one response to language in the fiscal 2004 Defense authorization bill that requires the department to make sure vulnerabilities in commercial software don't compromise military missions.** The proposed lab would create a single executive organization responsible for software integrity and information assurance.
Source: http://www.gcn.com/vol1_no1/daily−updates/25637−1.html

4. *April 19, Reuters* — **Pentagon to award billions in contracts.** The Pentagon is poised to award defense contracts valued at over $25 billion in the next few months, including a $6 billion deal to build the Army's next spy plane expected in early May. **Top U.S. defense firms are vying for major military jobs such as building a new U.S. Navy ship, a joint missile and a satellite communications system −− all of which focus on joint use by military services, communications and intelligence operations.** Loren Thompson of the Lexington Institute, a Virginia−based think tank, said the new weapons programs "are mostly about transforming the military by creating a networked force that does business in completely different ways." Many of the contracts, due in coming months, aim to bring U.S. military platforms into the high−speed information age.
Source: http://www.washingtonpost.com/ac2/wp−dyn?pagename=article&node=&contentId=A25141−2004Apr19&notFound=true

[Return to top]

Banking and Finance Sector

5. *April 20, Sydney Morning Herald (Australia)* — **Banks look for way to tighten online security. Representatives of some Australian banks held a meeting in Melbourne last week to discuss measures which could be adopted to provide better security for online banking.** The big four −− NAB, Commonwealth, ANZ and Westpac −− were represented at the meeting along with some of the smaller, regional banks. The meeting comes after a rash of phishing scams which have targeted the four big banks and also some of the smaller institutions −− last week Suncorp Metway was targeted while Bendigo Bank was a target in February. One of the solutions being considered is the use of security tokens that issue a one−time password which is valid for a single online session for each customer.
Source: http://www.smh.com.au/articles/2004/04/20/1082395833954.html

6. *April 19, Finextra Research* — **Surge in online phishing.** There has been a vast increase in the number of phishing e−mails in circulation over the past six months, according to online security services firm MessageLabs. Swiss bank Basler Kantonalbank is the latest to warn its customers of the scam e−mails, which claim to be from legitimate banks, but direct recipients to a replica Website where they are asked to enter personal security data that is used to make fraudulent online transactions. **MessageLabs says it recorded 279 scam e−mails in September 2003 but by March 2004 this figure had risen to 215,643.** The number of phishing e−mails peaked at 337,050 in January 2004. In North America, customers of TD Canada Trust, Citibank, Ebay's

PayPal and Visa have fallen for the scam. **Mark Sunner, chief technology officer, MessageLabs, claims the increase in the number of phishing e−mails is evidence that the number of individual scams has also risen dramatically.** "For targeted organizations, the impact can be high −− including lost productivity, customer confusion and complaints, damage to the brand and legal implications. If allowed to continue unchecked, online phishing scams threaten to undermine confidence in e−commerce as a whole," says Sunner.
Source: http://www.finextra.com/fullstory.asp?id=11640

7. *April 16, Boston Herald* — **Bank of America is reissuing Visa cards after hack attack. Holders of Fleet Visa business credit cards may be the latest victims of hackers who possibly got hold of sensitive card numbers via a merchant's computer system, officials acknowledged. Fleet Credit Card Services, now part of Bank of America Corp. after this month's takeover of FleetBoston Financial Corp., is sending new cards to customers because of a security breach at an unnamed merchant.** Deborah Pulver, the spokesperson, wouldn't say how many customers will get new cards and account numbers. Officials declined to say if the latest incident is tied to a recent theft of credit card numbers at Natick−based BJ's Wholesale Club Inc. On March 12, BJ's warned that a "few hundred" of its eight million members had their credit card numbers stolen in a possible systems breach. Richard Smith, an Internet security consultant in Brookline, said he knows no details about the BJ's and Fleet incidents. However, he said merchants in general are often the "weak link" in the credit−card security system. "The credit−card system has many players involved," he said, noting there have been infamous cases of Russian and Eastern European hackers stealing U.S. credit card numbers.
Source: http://business.bostonherald.com/technologyNews/view.bg?arti cleid=439

[Return to top]

Transportation Sector

8. *April 20, Associated Press* — **Los Angeles airport hit with second power outage in days.** Los Angeles International Airport suffered its second power outage in eight days, although flights were not disrupted thanks to backup batteries. A malfunctioning transformer was blamed for leaving some airport buildings without regular electricity for nearly two hours Monday, April 19. The cause of the electricity problems wasn't known. **"It's a little disturbing," said Bob Marks, regional vice president of the National Air Traffic Controllers Association. "This sure seems like a fragile power infrastructure."** Monday's blackout began at 11:31 a.m., causing lights to flicker in the airport. Although power returned immediately to some buildings, others remained on emergency lights until 1:19 p.m.
Source: http://www.cnn.com/2004/US/West/04/20/airport.blackout.ap/in dex.html

9. *April 20, Associated Press* — **Officials: Amtrak engineer caused train crash. The engineer of the Amtrak train that hit a Long Island Rail Road commuter train at Penn Station was responsible for the crash, which injured scores of people, the committee investigating the accident said Tuesday, April 20.** The Monday morning rush hour collision "was caused by human error on the part of the engineer of Train 183, the Amtrak train," Amtrak spokesman Dan Stessel said. "You must be able to stop your train short of another train," Stessel said. The engineer, whose identity was withheld by Amtrak, has been suspended without pay. Stessel said

a formal investigation is pending and further action may be taken based on the outcome of that effort. Amtrak was awaiting the results of drug and alcohol tests. The investigating committee was made up of Amtrak, LIRR and federal railroad officials.
Source: http://www.newsday.com/news/local/newyork/nyc−crash0421,0,2300733.story?coll=ny−nynews−headlines

10. *April 19, Baltimoresun.com* — **Better intelligence needed to protect port.** Acknowledging that new fences lining the port of Baltimore aren't enough to stop a terrorist's bomb from reaching the shores of Maryland, federal and state officials said Monday, April 19, that the emphasis in protecting the waterfront will shift to better intelligence work. **Various agencies will have to cooperate in an unprecedented fashion to thwart threats from chemical, biological or nuclear weapons before they sail into Baltimore or any of the nation's other 360 ports, said the officials, who briefed members of Congress Monday at the port about their progress.** The Baltimore region has received about $14 million in state and federal money that went toward a patrol boat, fencing and new technology. An undetermined fourth round of dollars will available soon. The new technology will include a better tracking system to monitor cargo on each vessel coming into the port and X−ray machines to see inside containers that are flagged as suspicious. On average, about six percent of containers are now inspected by U.S. Customs officials at ports nationwide. But Rep. Benjamin L. Cardin, the Baltimore Democrat, said he believes Baltimore's average is higher, although the number varies depending on the perceived threats.
Source: http://www.baltimoresun.com/news/custom/attack/bal−port0419,0,7257311.story?coll=bal−home−headlines

11. *April 19, Info−Prod Research (Middle East)* — **Moscow to boost security in the Metro. The Duma's Security Committee on April 16, authorized a two−year, 2.5 billion−ruble ($87 million) program to install metal detectors and gas−detection equipment in all tunnels and stations of the Moscow subway system,** gzt.ru and newsru.com reported on 19 April. The program will also include the creation of a passenger−safety unit within the subway. Last month, Moscow subway Director Dmitrii Gaev announced that within two years all 4,221 subway cars in the system will be equipped with video−surveillance cameras.
Source: http://cnniw.yellowbrix.com/pages/cnniw/Story.nsp?story_id=50039448&ID=cnniw&scategory=Transportation:Mass+Transit&

[Return to top]

Postal and Shipping Sector

12. *April 20, Federal Computer Week* — **Postal Service uses software to manage labor pool.** In Philadelphia, 2,500 U.S. Postal Service (USPS) employees work in a mail−processing facility that stretches across five floors. Three floors in an adjacent truck terminal and a nearby rail yard hum with other mail−sorting activities day and night. **The Philadelphia facility and others like it present a challenge for USPS workforce managers: how to assign the right workers to the right place at the right time. To deal with the problem, managers have begun using optimization software, known as the Labor Force Schedule Optimizer System.** Under pressure to cut costs and offer better service, facilities managers say the planning tool has helped them operate more efficiently at several test sites. In 2001, when USPS officials first

used the planning tool in a series of pilot and proof−of−concept tests, they eliminated 1,600 full−time equivalent positions out of 11,500. Now that operations managers are using the tool in at least 19 postal plants, managers expect to begin scheduling mail−processing work more efficiently in those facilities. **By spending $14.6 million on optimization software, USPS officials expect to eliminate excess labor costs and save $135 million.**
Source: http://www.fcw.com/fcw/articles/2004/0419/mgt−postal−04−19−0 4.asp

[Return to top]

Agriculture Sector

13. *April 20, Associated Press* — **High grain costs worry livestock producers.** As grain farmers look forward to profitable crops because of high corn and soybean prices, livestock producers worry it could mean a big jump in their expenses. **Corn at three dollrs per bushel and soybean meal prices of about $300 per ton are raising the cost to feed a hog by four to five dollars for every 100 pounds of animal, said Art Lehman, president of the Illinois Pork Producers Association.** Live hogs are selling in the $52 per hundredweight range, which lessens the blow a bit. But futures prices indicate that number could drop to the 40s by fall. About $43 per hundredweight is the break−even price for a hog, Lehman said. "If we get lower prices and still have three dollar corn it's going to be a real pinch for a lot of people," he said. **The higher grain prices also are raising costs for beef producers, but the cattle market is good, with prices near $80 per 100 pounds, said Curt Rincker, president of the Illinois Beef Association.** "If we have any problems with the growing season and grain prices continue to stay high, I think you probably will see some adjustments," said Dale Lattz, a farm management specialist at the University of Illinois. "People will look at their operations more closely."
Source: http://www.mlive.com/newsflash/business/index.ssf?/base/busi ness−18/1082451631271530.xml

14. *April 20, Reuters* — **USDA won't pay whole cost of ID system. The U.S. government may pay about one−third the estimated $550 million cost to set up an animal identification system, an U.S. Department of Agriculture (USDA) official said on Monday, April 19, providing the first outline of the government's financial commitment to the program.** Chief economist Keith Collins also said he believed USDA was close to gaining White House approval to dip into emergency funding so it can launch the nationwide ID plan this year. Agriculture Secretary Ann Veneman announced four months ago that implementation of a nationwide animal identification plan would be speeded up. The goal would be to identify within 48 hours the herdmates of suspect animals when there is a disease outbreak. **USDA wants to begin issuing ID numbers later this year to farms, ranches, feed lots, packing plants, and other places where animals congregate.** It might even be able to begin issuing ID numbers to individual animals or groups of animals by the end of the year, Collins said. The Bush administration has requested $33 million for animal ID work in fiscal 2005, beginning October 1.
Source: http://www.agriculture.com/default.sph/AgNews.class?FNC=Mons entoDetail__ANewsindex_html___51624

[Return to top]

Food Sector

15. *April 19, Oster Dow Jones Commodity News* — **U.S. to allow bone−in beef from Canada. As of Monday, April 19, the U.S. and Canada have opened up the trade to bone−in beef so long as it is from cattle that are under 30 months of age, according to U.S. Department of Agriculture (USDA) Undersecretary Bill Hawks.** Hawks said that Canadian exporters will still have to get permits to export the beef products to the U.S. Hawks stressed that this decision has nothing to do with the live cattle rule now being considered by the USDA. That proposed rule would also allow in Canadian beef from cattle that are over 30 months of age. The comment period for cattle import rule closed recently, but USDA officials have refused to speculate on how long the review will take. Hawks also said some ground beef products are coming into the U.S. but that was not considered a new development.
Source: http://www.agprofessional.com/show_story.php?id=24611

[Return to top]

Water Sector

16. *April 19, Water Tech Online* — **Water grants awarded by EPA.** The U.S. Environmental Protection Agency (EPA) has awarded states, territories, and tribes their shares of FY2004 grants to support state drinking water programs. The grants are part of the Drinking Water State Revolving Funds (DWSRF). **Total funds appropriated by Congress for the current fiscal year amounted to $102 million for state Public Water System Supervision (PWSS) grants and $845 million for the DWSRF account.** Of the total PWSS grant pot, EPA reserved $6.6 million to support tribal programs, leaving $95.4 million to split among states and U.S. territories. Of the total DWSRF appropriation, EPA set aside $12.7 million for American Indian and Alaska Native Villages programs and two million dollars to support monitoring of unregulated contaminants under the Unregulated Contaminants Monitoring Rule, leaving $830.3 million for states, the District of Columbia, and U.S. territories.
Source: http://www.watertechonline.com/news.asp?mode=4&N_ID=47142

[Return to top]

Public Health Sector

17. *April 20, Los Angeles Times* — **New York man infected with bird flu. Health officials have confirmed that a Westchester County, New York, man was infected with a strain of flu that normally affects birds, only the second such case reported in the United States.** The man reported to Westchester Medical Center in November with symptoms including fever and cough. Doctors tentatively identified a human flu strain in sputum samples taken from the man, but sent the samples to the U.S. Centers for Disease Control and Prevention (CDC) for confirmation. Scientists at the CDC said in March they had identified the virus as H7N2, a strain of avian flu. The identification was confirmed April 16 after the man's blood was tested for antibodies, **The diagnosis raised questions because the man apparently did not work with birds or poultry, health officials said.** The patient in the only known previous human

case of avian flu in the U.S. was a poultry worker in Virginia. **"We can't figure out how he was exposed and why he's an isolated case," CDC influenza expert Nancy Cox said. "We need to understand how he got infected."**
Source: http://www.latimes.com/news/nationworld/nation/wire/ats−ap_health13apr20,1,4915585.story?coll=sns−ap−tophealth

18. *April 20, Medical News Today* — **Few new antibiotics are in the pipeline. Despite a critical need for new antibiotics to treat drug−resistant infections and other infectious diseases, very few new antibiotics are being developed, according to a study.** To document trends, researchers evaluated Food and Drug Administration (FDA) databases of approved drugs and the research and development (R&D) programs of the world's largest pharmaceutical and biotechnology companies, by looking at the companies' websites and 2002 annual reports. **They found that FDA approvals of new antibiotics declined 56 percent during the past 20 years (1998−2002 versus 1983−1987).** Looking to the future, the researchers found only six new antibiotics in the R&D pipeline out of 506 drugs being developed. Bacteria, which are treated with antibiotics, are by far the most common cause of infectious−related deaths in the United States. **Because of the emergence of drug−resistant bacteria, the researchers note that there are few or no treatment options for many infections.**
Source: http://www.medicalnewstoday.com/index.php?newsid=7452

19. *April 19, National Institutes of Health* — **Second vaccine candidate helps mice fend off SARS. An experimental vaccine based on a critical piece of the Severe Acute Respiratory Syndrome (SARS) virus protects mice from SARS infection, researchers from the National Institute of Allergy and Infectious Diseases (NIAID, have found. When exposed to the SARS virus, immunized mice produced SARS−specific antibodies, and virus replication was nearly eliminated.** The new report is the second from NIAID in recent weeks describing a promising SARS vaccine candidate. "We now have two candidate vaccines, based on two distinct technologies, shown to be effective against SARS infection in mice," said NIAID Director Anthony S. Fauci. "The animal model employed in both studies was developed by NIAID researchers as well. By taking various approaches to vaccine development, we are making significant research progress against a disease that was unknown little more than a year ago."
Source: http://www.nih.gov/news/pr/apr2004/niaid−19.htm

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

20. *April 20, NBC 4 News (Los Angeles, CA)* — **$2.5 million oil spill exercise under way.** The largest multi−agency training exercise in U.S. history in dealing with oil spills will take place Tuesday through Thursday in Southern California and Mexican waters, according to the U.S.

Coast Guard. **The $2.5 million drill −− which includes the Coast Guard, state Fish and Game, American Petroleum Institute Consortium and the Mexican government −− involves a simulated crude−oil tanker explosion near Los Angeles. The exercise also will involve a simulated collision near San Diego, according to U.S. Coast Guard Chief Warrant Officer Lance Jones.** "This exercise is an important opportunity for us to work in a unified response effort to protect the public, environment and economic resources in the event of a major spill," USCG Vice Adm. Terry M. Cross, commander of the Pacific Area, said earlier this month. Command posts will be set up in San Diego, Los Angeles, Los Alamitos and in Ensenada, Mexico. The Department of Homeland Security's Initial Response Team will participate in the drill, the first of the kind for the newly created unit, officials said. The latest cleanup technology will be used during the three−day drill. The Oil Pollution Act of 1990 requires such exercises.
Source: http://www.nbc4.tv/news/3022929/detail.html

21. *April 20, Associated Press* — **Gov. Wise gives $31.1M for security.** To help local communities and the state prepare for terrorist attacks and weapons of mass destruction assaults, West Virginia Gov. Bob Wise on Monday, April 19, gave out $31.1 million in federal grants. **Grants for equipment ranging from software and patrol boats to chemical decontamination units and hydraulic jacks for urban rescues, along with cash grants for planning and training, will be sprinkled across all 55 counties as well as 21 cities and 10 state agencies.** "It,s a tremendous thing when we can do something that helps our police officers, firefighters and other emergency responders," Wise said. "The distribution of this money will further enhance our homeland security efforts." Those grants are being distributed among six regions the state has created to speed emergency response times while ensuring that responder equipment, from radios to airpacks, is interchangeable and not needlessly duplicated.
Source: http://www.herald−dispatch.com/2004/April/20/LNlist4.htm

22. *April 19, Government Executive Magazine* — **Scientists to simulate chem−bio attack around Pentagon.** Aiming to protect Pentagon employees from chemical or biological attacks, government scientists on Monday, April 19, began collecting atmospheric data throughout the 583−acre Pentagon reservation. **To simulate how chemical and biological agents would flow around and into the Pentagon, scientists will release sulfur hexafluoride, SF6, a commonly used agent in airflow testing. The colorless, odorless gas is deemed so safe that it is approved by the Food and Drug Administration for injection into the body for specialized tests, according to the Pentagon.** The Environmental Protection Agency and the Virginia Department of Environmental Quality have approved the testing protocol. The atmospheric survey, dubbed Pentagon Shield, will use standard weather sensors mounted on light poles around the Pentagon, on the building roof and in the center courtyard to measure wind speeds, direction and temperature. The survey data will be used to improve computer modeling that simulates atmospheric conditions around the Pentagon and eventually will contribute to the development of chemical/biological surveillance systems that can be used to protect other facilities, Flood says.
Source: http://www.govexec.com/dailyfed/0404/041904kp1.htm

[Return to top]

Information and Telecommunications Sector

23. *April 20, eWEEK* — **WorldCom emerges from bankruptcy. WorldCom Inc. officially changed its name to MCI Inc. Tuesday, April 20, as it completed its emergence from Chapter 11 bankruptcy protection**. The company, dragged down by approximately $11 billion in accounting fraud and the largest bankruptcy in U.S. history, is reinventing itself with a redoubled focus on secure data and integration services. The company will center its efforts on providing converged data and voice services to the business and government markets, leveraging its global IP networking assets. MCI plans to act increasingly as a services integrator for enterprise customers, and will soon announce new security offerings, Michael Capellas, president and CEO, said Tuesday. The second largest long−distance carrier does not hold cellular telephone frequencies and does not plan to offer wireless services directly, but the company sees an opportunity in integrating other carriers' offerings and providing security for them, allowing customers to use multiple carriers, Capellas said. **With the completion of the bankruptcy process, which allowed the company to eliminate $36 billion in debt, MCI has begun distributing securities and cash to its creditors.**
Source: http://www.eweek.com/article2/0,1759,1570745,00.asp

24. *April 20, Washington Post* — **Experts race to fix serious Internet flaw.** Computer security experts in the U.S. and UK confirmed Tuesday, April 20, that **a new method has been identified that could make it easy for hackers to disrupt Internet communications worldwide. The exploit, identified by Milwaukee security researcher Paul Watson, could give hackers the ability to crash Internet routers**−−the complex machines that direct most of the world's Web traffic. Watson's method takes advantage of an inherent design flaw in transmission control protocol (TCP)−−the language that all computers use to communicate on the Internet−−that could place ordinary computers at greater risk of attack. **Watson is slated to present his findings at a security conference in Canada later this week.** Amit Yoran, director of the cybersecurity division for the Department of Homeland Security, said most of the world's major Internet service providers had already taken steps to prevent the attack. Additional information is availabe in "Technical Cyber Security Alert TA04−111A: Vulnerabilities in TCP," available on the U.S. Computer Emergency Readiness Team Website: http://www.us−cert.gov/cas/techalerts/TA04−111A.html. The UK's National Infrastructure Security and Coordination Center has posted a vulnerability notice here: http://www.uniras.gov.uk/vuls/2004/236929/index.htm
Source: http://www.washingtonpost.com/wp−dyn/articles/A27890−2004Apr 20.html

25. *April 19, Federal Computer Week* — **Last part of security strategy released.** A cybersecurity task force organized by the National Cyber Security Partnership issued a 104−page report with recommendations for the federal government and industry on Monday, April 19. The report is the last of five documents prepared by industry and academic experts on the President's National Strategy to Secure Cyberspace, a general blueprint for improving the nation's cybersecurity readiness. **The task force members called for what they said were needed improvements to the consumer− and vendor−oriented software security testing program** operated by the National Institute of Standards and Technology and the National Security Agency. The report recommends that NIST receive an initial $12 million in new appropriations and $6 million in following years for developing security requirements for specific classes of products such as intrusion−detection systems and virtual private networks. **Other steps outlined in the report include making vendors responsible for shipping software products**

with more of their security features enabled and having the federal government mandate software−vulnerability analysis as a condition of procurement. The group also recommended that industry groups work together to develop a well−defined set of technical standards for designing secure IP networks. The report is available online: http://www.cyberpartnership.org/TF4TechReport.pdf
Source: http://fcw.com/fcw/articles/2004/0419/web−ncsp−04−19−04.asp

26. *April 19, InformationWeek* — **DHS needs public−private cooperation.** Speaking at the Information Security Decisions conference in New York on Monday, April 19, Amit Yoran, director of the Department of Homeland Security's National Cyber Security Division, noted the challenges associated with this need for public−sector agencies and private−sector companies to coordinate their knowledge of cyberthreats and physical threats, as well as infrastructure vulnerabilities. **DHS estimates that private−sector companies run 85% of the services required to ensure national security, public health and safety, and economic stability. Yet private−sector executives are reluctant to provide critical infrastructure information about their companies' operations for fear of their vulnerabilities becoming a matter of public record**. Software quality is also a key issue for cybersecurity−−particularly because most software users aren't security experts. Developers must address the most obvious problems. "Ninety−five percent of software bugs are caused by the same 19 programming flaws," Yoran said. And **software quality will only become more difficult to police as more and more is developed by foreign nationals both offshore and within the United States**, Yoran said. Companies will have to be on guard against backdoors potentially written into software that could allow access to their systems.
Source: http://www.informationweek.com/story/showArticle.jhtml?artic leID=18902167

27. *April 19, eSecurity Planet* — **FTC urges industry solutions to spyware. The Federal Trade Commission (FTC) says the solution to the invasive programs generally known as spyware is more likely to be found in better technology solutions and intensive consumer education than in either state or federal legislation**. Spyware is vaguely defined and often confused by consumers with adware, which are usually legal and legitimate applications. Consumer and privacy advocates attending Monday's FTC Spyware Workshop were concerned about the growing number of programs that often surreptitiously piggyback on downloaded files; they report back Internet traffic patterns to advertisers and generate unwanted popups. Even when consumers delete the downloaded file, spyware often remains and continues to monitor the user's browsing habits. FTC Commissioner Mozelle Thompson asked industry Internet provider leaders to produce a set of best practices for the use of adware, including disclosure statements to consumers regarding what they are about to download.
Source: http://www.esecurityplanet.com/trends/article.php/3342471

Internet Alert Dashboard

Current Alert Levels

AlertCon: 2 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **HTML_NETSKY.P** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 80 (www), 445 (microsoft−ds), 2745 (urbisnet), 3127 (mydoom), 137 (netbios−ns), 1433 (ms−sql−s), 139 (netbios−ssn), 1025 (blackjack), 4899 (radmin) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

28. *April 20, Reuters* — **Italy seizes assault rifles headed to U.S.** Italian customs officers seized more than 8,000 Kalashnikov assault rifles and other weapons on a ship headed to the United States, officials said Tuesday, April 20. **The arms, worth about $7.15 million, were discovered aboard a ship arriving from Romania that pulled into the southern Italian port of Gioia Tauro on its way to the United States,** Italy's customs said in a statement. According to the travel documents, the arms belong to a large U.S. company with headquarters in the state of Georgia. The arms were found inside three containers during a routine customs check earlier this week. They were confiscated due to discrepancies in the customs forms. The customs office said the weapons had been described as "common guns" instead of assault rifles and longer−range combat arms in the travel documentation.
Source: http://abcnews.go.com/wire/US/reuters20040420_229.html

29. *April 20, Associated Press* — **Terror fears after gas tanker disappears from parking lot. A gasoline tanker truck has been missing from a Pennsauken, NJ, parking lot for more than a week. The New Jersey Office of Counterterrorism has asked all the state's law enforcement agencies to look for the truck.** "We don't know what the motive was behind the theft," FBI spokesperson Linda Vizi said. "It could have been stolen by another individual in the fuel−hauling business. But we feel it's important to find it, find out who took it, and find out why it was taken." The recently refurbished 1996 Fruehauf tanker, with "TK Transport" in large green letters on its side and the New Jersey license plate number T852SC, was last seen April 8, said Pennsauken Police Capt. Earl Griffin. However, Griffin said it was a few days before workers at the TK Transport Terminal noticed it was gone. **Griffin said he's been in touch with TK Transport to try to make sure the truck is missing because it was stolen and not simply because of a communication foul−up. Griffin said the truck did not have any liquid in its chrome−plated tank.**
Source: http://www.wnbc.com/news/3022869/detail.html

30. *April 20, CNN* — **Terror arrests in Sweden. Swedish National Police say they have arrested four people to question them in connection with terrorist activities. According to authorities, the four detained are associated with Islamic extremist groups, but their activities do not concern Europe.** "We can confirm that four people have been arrested and questioned," SAPO spokesman Robert Dahlberg told The Associated Press. "They are suspected of having connections to terrorist activities, Islamic extremism." All are four are being detained by police for more questioning, Dahlberg said. **The four men were not identified were arrested in separate operations in the capital, Stockholm, and in the southwestern city of Malmoe on Monday, April 19.** Dahlberg said none of the four were involved in any terror attacks in Europe.
Source: http://edition.cnn.com/2004/WORLD/europe/04/20/sweden.terror .arrests/index.html

31. *April 20, Local6.com (Central Florida)* — **Brush fire threatens homes in Orange County.** A brush fire that was possibly man−made in Orange County, FL, forced the evacuation of about 40 homes Monday night, according to Local 6 News. Fire officials said flames came within 10 feet of homes in the Hunter's Creek area of Orange County. Authorities said residents living on two streets in two different subdivisions were evacuated. A resident filmed the 15−acre fire as it approached his subdivision before the evacuations. **The cause of the fire is under investigation but the fire appeared to be man−made, Local 6 News reported.** About 10 fire units were called to fight the blaze, according to the report. There was no damage to homes and no reported injuries. The fire was brought under control just before midnight.
Source: http://www.local6.com/news/3021353/detail.html

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at info@us−cert.gov or visit their Web page at www.uscert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.